# SECURITY THREATS IN CLOUD COMPUTING ENVIRONMENT

*SHAVETA DARGAN*

**Assistant Professor in Computer Science, Guru Nanak College for Girls, Sri Muktsar Sahib, Punjab University Chandigarh**.

***ABSTRACT**: Today the world is using one of the most evolving and growing technology in the computing environment – Cloud Computing. Cloud computing has changed everybody's vision. Cloud computing is a technology which is built on the virtualization, grid computing, distributed computing. There are number of models such as Software as a Service (Saas), Platform as a service (Paas), Infrastructure as a Service (Iaas) by which cloud computing is providing services to the cloud user and a large number of cloud service providers are available world wide. But the serious limitation with cloud computing is its security. The paper begins with the introduction and architecture of cloud computing. Then the main focus is on the security threats of cloud computing and the countermeasures for the security problems. At the end there is conclusion and research challenges in this paradigm.*

***Keywords: Cloud Computing, cloud service user, cloud service provider, virtualization, grid computing, distributed computing.***

## 1. INTRODUCTION:

Cloud computing is the first among top 10 most important technologies and with a better prospect in the successive years. Cloud computing is an internet based computing which relies on sharing of the resources such as server, storage, applications through internet and the goal is to provide high performance computing. Cloud computing incorporates virtualization, on demand deployment, internet delivery of services and open source software. The three important characteristics that differentiate cloud computing from others are on demand, elastic and the service is managed by the provider. A cloud can be public cloud (which provide services to anyone on the internet) such as Amazon and the private cloud (provide limited services) such as data centers.

There is no doubt that the convenience and low cost of cloud computing services have changed our daily lives; however, the security issues associated with cloud computing make us aware to cyber crimes. Hackers use a variety of techniques to gain access to clouds without legal authorization in order to achieve specific objectives and therefore gaining unauthorized access to the information stored in the cloud. Once the exact location of data is located, hackers steal private and sensitive information for criminal activities. Therefore, it is necessary to have a good understanding of cloud security policies in order to provide more secure services to cloud users.

## 2. CLOUD COMPUTING ARCHITECTURE:

It is the structure which comprise on premise cloud resources, services, middleware and the software components. The architecture of cloud computing includes three layers: the System layer, the Platform layer and the Application layer.

▪ The bottom layer is the system layer, which includes computational resources such as infrastructure of servers, network devices, memory, and storage. It is known as Infrastructure-as-a-service (IaaS). The computational resources are made available for users as on-demand services. With the use of virtualization technology, IaaS provides virtual machines that allow clients to build complex network infrastructures. The advantage of this service is to have reduced cost and ease the load of network administration. An example of a cloud computing service provider of IaaS is Amazon's EC2.

▪ The middle layer is the platform layer and is known as Platform-as-a-Service (PaaS). This layer provides a development platform for users to design their specific applications. Services provided by this cloud model include tools and libraries for application development so that users have control over the application deployment and configuration settings. With PaaS, developers are not required to buy software development tools, therefore reducing the cost. GoogleApps is an example of PaaS. Windows Azure is another PaaS provider.

▪ Finally, the top layer is the application layer, also known as Software-as-a-Service (SaaS). This layer allows users to rent applications running on clouds. Because of its ability to reduce costs, SaaS is popular among companies that deploy their businesses. Groupon is an example that uses SaaS.

The cloud computing service providers on the cloud service models are:

1. Saas: CVM Solutions Cloud9 Analytics, Google Apps, IBM, Antenna Software.
2. Paas: Amazon AWS, Google Apps, Microsoft Azure, Sales force, WorkXpress.
3. Iaas: Amazon Elastic Compute Cloud, Rackspace, Bluelock, GoGrid.

## 3. CLASSIFICATION OF SECURITY THREATS IN CLOUD COMPUTING ENVIRONMENT:

Three cloud service models (SaaS, PaaS and IaaS) not only provide different types of services to end users but also reveal security issues and risks of cloud computing systems.

➢ **Misuse of computational resources**: The hackers might misuse the computing capability provided by clouds by conducting illegal activities. IaaS is present in the bottom layer, which directly provides the most powerful functionality of an entire cloud. It maximizes the capability for users to customize a "realistic" environment that includes virtual machines running with different operating systems. Hackers could rent the virtual machines, analyze their configurations, find their vulnerabilities, and attack other customers' virtual machines within the same cloud. IaaS also enables hackers to perform attacks, e.g. brute-forcing cracking. Since IaaS supports multiple virtual machines, it provides an ideal platform for hackers to launch attacks that require a large number of attacking instances.

➢ **Data loss**: Data loss is an important security risk of cloud models. In SaaS cloud models, companies use applications to process business data and store customers' data in the data centers. In PaaS cloud models, developers use data to test software integrity during the system development life cycle (SDLC). In IaaS cloud models, users create new drives on virtual machines and store data on those drives. However, data in all three cloud models can be accessed by unauthorized internal employees, as well as external hackers. The internal employees are able to access data intentionally or accidentally. The external hackers gain access to databases in cloud environments using a range of hacking techniques such as session hijacking and network channel eavesdropping.

➢ **Data Breaches**: Security threats can occur from both outside the organization and within the organization. The most common inside attack were unauthorized access to and use of corporate information. These inside attacks generally occur due to unclear responsibilities and roles, inadequate physical security procedures, rogue administrator, exploitation of cloud vulnerabilities. Secondly the sensitive data present on the cloud become the target to online cyber theft. E.g. online retailer Zappos was the victim of online cyber theft. Also the Linked In the world largest professional working website that has 175 million users reported that their password database was compromised in a security breach. Dropbox has also confirmed that its users suffered from a spam attack.

➢ **Loss of Governance**: For a business enterprise, migrating its own IT system to cloud infrastructure means giving partial control to cloud service providers. This loss of governance depends on the cloud service models.

➢ **Protection inconsistency**: Due to decentralized architecture of cloud infrastructure, its protection procedures are inconsistent among security models.

➢ **Insecure Application Program Interface**: Cloud service providers expose a variety of interfaces to the cloud users to manage and interact with the cloud services. The security and availability of cloud services is dependent on the security of the API's. So it is necessary to design these interfaces in such a way so as to protect from both accidental and malicious attacks.

➢ **Account or service hijacking**: Account or service hijacking is not a new concept but cloud solutions add something to it. Suppose if an attacker gains access to our credentials, he can eavesdrop our activities, manipulate the data and redirect the client to illegitimate sites and hence our account become the base for the attacker.

➢ Traditional network attack strategies can be applied to harass three layers of cloud systems. For example, web browser attacks are used to exploit the authentication, authorization, and accounting vulnerabilities of cloud systems. Malicious programs (e.g. virus and Trojan) can be uploaded to cloud systems and can cause damage. Malicious operations can be embedded in a normal command, passed to clouds, and executed.

## 4. COUNTERMEASURES FOR THE SECURITY THREATS:

As the number of security threats in cloud computing environment is reaching height day by day and keep focusing the popularity and use of cloud computing technology, it is mandatory to have some countermeasures for the security threats. Also to have the best quality of service, the providers are responsible for ensuring the cloud environment is secure. The following are some solutions to the security problems:

➢ **Security Policy Enhancement**: It is easy to register in the cloud and utilize the services offered by the cloud service provider by using valid credit card. So hackers can take the advantage and can do malicious activities such as spamming and attacking other computing systems. This is only possible if the registration system is weak. So to implement security policies and well established rules and regulations it is possible to manage the clouds more effectively.

➢ **Data Protection**: There are varieties of security tools that are available to control the behavior of insiders such as data loss prevention systems, anomalous behavior pattern detection tools, format preserving and encryption tools, decoy technology, authentication and authorization technologies and user behavior profiling. These tools provide the functions for real time detection on monitoring traffic and trapping malicious activities of hackers into decoy documents.

**Access Control**: It is a mechanism or a tool to ensure authorized user can access and to prevent unauthorized access to information system. Special attention must be given to control the allocation of privileged access rights. For proper access control management, there must be controlled access to information, operating system, applications, network services and management of user access rights.

- **Partitioning:** To distribute the workload among multiple computing nodes, it is important to divide the data into partitions that can maximize transactions and have good query response.
- **Migration:** One of the main demands for the cloud computing is flexibility which means dedicating resources where they are most needed. In migration, available method must predict adaptation time and try to minimize the overloading of the nodes.

## 6. CONCLUSION AND RESEARCH CHALLENGES:

It is undoubtedly said that cloud computing is providing benefits to IT enterprises with its various facilities and on demand services in a cost effective manner. But there are various challenges and security problems which everyone must consider before transferring the data to a cloud. So the key to better quality of service and successful cloud computing initiatives is to have balance between benefits and the risks associated. Cloud providers should add more resources and security policies to protect themselves from malicious attacks. In this paper we discussed the architecture, classification of security threats and the solutions at the last for these problems. As the cloud computing is in continual development so the researchers have a lot of challenges in handling the security threats, energy resource management, interoperability and reliability in cloud computing and make it a successful technology.

## 7. REFERENCES:

[1] Kangchan Lee, “Security Threats in Cloud Computing Environment”, International Journal of Security and its Applications, Vol. 6, No. 4, October 12.

[2] Keiko Hashizume, David G Rosado, “An Analysis for Security Issue for Cloud Computing”, Journal of Internet Services and Applications, 2013.

[3] Te-Shun Chou, “Security Threats on Cloud Computing Vulnerabilities”, International Journal of Computer Science and Information Technology, Vol. 5, No. 3, June 2013.

[4] “Top threats to Cloud Computing V1.0, Cloud Security Alliance”, March 2010.

[5] Farzad Sabahi, “Cloud Computing Security Threats And Responses”, IEEE 2011.

[6] The Notorious nine, Cloud Computing Top Threats in 2013, Cloud Security Alliance, 2013.

[7] Rabi Prasad Padhy, Manas Ranjan Patra, Suresh Chandra Satapathy, “Cloud Computing: Security Issues and Research Challenges”, International Journal of Computer Science and Information Technology and security, Vol1, No. 2, pp. 136-146, December 2011.

[9] Puja Dhar, “Cloud Computing and its Applications in the world of networking”, International Journal of Computer Science, Vol. 9, Issue 1, No. 2, pp 430-433, January 2012.

[10] Stayender Singh Rawat, Alpesh Soni, “A Survey of Various Techniques to Secure Cloud Storage”, National Conference on Security Issues in Network Technologies, Aug 11-12, 2012.

[11] Mladen A. Vouk, “Cloud Computing- Issues, Research and Implementations, Journal of Computing and Information Technology-CIT 16, 2008,4, pp. 235-246.

[12] Vahid Ashtorab, Seyed Reza Taghizadeh, “Security threats and Countermeasures in Cloud Computing, International Journal of Application or Innovation in Engineering & Management, vol. 1, Issue 2,pp. 234-245, October 2012.